respective AAA services, they will receive that address. This is done by returning the IP address in the access-accept packet ultimately returned to the NAS via the PGW.

For users of the local ISP who do not have pre-allocated IP addresses, a DHCP (dynamic host control protocol) service such as one running in a host at the PoP will provide a DHCP IP address from a pool of such addresses assigned to the ISP.

For wholesale users, an IP address may be returned from a DHCP service running remotely at their provider, it may be assigned by the ISP as if the user were a retail user of the ISP, or a separate pool of IP addresses maintained locally at the ISP on behalf of the provider can be identified by the access-accept packet and an address selected therefrom by the local DHCP service.

Turning now to FIGS. 9–12, FIG. 9 is a flow diagram detailing the process whereby the AAA service and its database at a PoP are instantiated. The AAA service is preferably started (100) with a command entered at the NCC 12 within NOC 16. The start command is passed over information bus 22 to information broker 24 which publishes it to subscribing entities such as a control adapter at the PoP. The control adapter responds by starting the process. Once the process is started a configure command at the NCC causes publication (102) of database elements which are used to populate (104) the database of the AAA service at the PoP. This is preferably done using the broker-publisher mechanism described above with the AAA service or its database being the subscriber to the published information. FIG. 10 details a similar process for loading the database of a proxy or GRS server at the PoP.

FIG. 11 details the process whereby a user is authenticated and authorized in accordance with a presently preferred embodiment of the present invention. At reference numeral 112 the user attempts a log-in by dialing in to a NAS at the PoP. At reference numeral 114 the network access request from the NAS is forwarded to a protocol gateway for processing. At reference numeral 116 the protocol gateway parses the FQDN of the user. If the FQDN indicates that the user's domain is processed directly at the PoP's AAA service, then the access request is forwarded there (118). Processing proceeds in a conventional manner. If the FQDN indicates that the user is to be authenticated remotely, then at reference numeral 120 the protocol gateway forwards the network access request to a proxy server or GRS server at the PoP for proxy processing. At reference numeral 122 the proxy/GRS server looks up the user's domain AAA contact information (e.g., address, port number) from the database associated with the proxy/GRS server and populated as described above. At reference numeral 124 the proxy/GRS server proxies the access request to the now-identified remote AAA service at the user's domain site. Processing proceeds in a conventional manner from this point on.

FIG. 12 details the flow of the process by which the protocol gateway may load balance among multiple instantiations of AAA services and/or GRS/proxy services. At reference numeral 126 the protocol gateway maintains a database indicative of the responsiveness of the various AAA services and proxy/GRS services with which it is in contact at the PoP. Since it is sending requests to the services all the time as users attempt to log-in, and because the service must acknowledge receipt of the requests in a conventional manner, it is a simple matter to determine the response time of the service at any given moment. Also, since the protocol gateway is feeding all of the access requests to their respective services, it is simple to track how many are being forwarded at any given time at the PoP.

At reference numeral 128 the protocol gateway load balances by distributing network access requests among the relevant services in a manner designed to more or less equally share the load. Any convenient mechanism may be used, such as a round-robin schedule or another conventional scheduling algorithm.

At reference numeral 130 the protocol gateway detects non-responsive services and bypasses them. An error condition event may also be published to allow other components of the data communications network to become aware of the failure.

Turning finally to FIG. 13 a flow diagram of a process whereby accounting event records are distributed is shown. At reference numeral 132 an accounting event is detected. This could be, for example, an accounting start event or an accounting stop event detected at the protocol gateway. At reference numeral 134 the nature of the connection is determined. If it is a local user of the PoP, then the accounting event information is sent only to the local AAA service at reference numeral 136. If it is a proxy user, then at reference numeral 138 the accounting event is sent both to the local AAA service as well as to the proxied AAA service.

Alternative Embodiments

While embodiments and applications of the invention have been shown and described, it would be apparent to those of ordinary skill in the art, after a perusal of the within disclosure, that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.

What is claimed is:

1. A method for managing network access to a data communications network, said method comprising:

maintaining a central database;

maintaining at least one authentication, authorization and accounting (AAA) service at a point of presence (PoP) of the data communications network; and

configuring a database associated with the AAA service from the central database, wherein said configuring includes publishing information from said central database on an information bus as at least one event, said AAA service subscribing to said event so as to receive said published information so as to thereby update its associated database.

2. A method in accordance with claim 1, further comprising:

receiving at a protocol gateway in the PoP a network access request from a user through a network access server (NAS);

parsing the network access request for an identification of the user's domain;

routing the network access request to the AAA service at the PoP if the user's domain corresponds to that of the PoP;

looking up a domain identification entry corresponding to the user's domain in the AAA service's database if the user's domain does not correspond to that of the PoP;

proxying the network access request to an AAA service in the user's domain at an address and port as specified in the domain identification entry of the database if the user's domain does not correspond to that of the PoP.

3. A method in accordance with claim 2, further comprising:

obtaining an IP address for the user from the AAA service in the user's domain if the user's domain does not correspond to that of the PoP.

4. A method in accordance with claim 2, further comprising:

assigning an IP address to the user from a local DHCP pool of IP address if the user's domain does not correspond to that of the PoP.

5. A method in accordance with claim 2, further comprising:

assigning an IP address to the user from an IP address pool identified in an access-accept packet received from the user's domain's AAA service if the user's domain does not correspond to that of the PoP.

6. A method for managing network access to a data communications network, said method comprising:

maintaining a central database;

maintaining a plurality of authentication, authorization and accounting (AAA) services at a point of presence (PoP) of the data communication network; and

configuring databases associated with the AAA services from the central database, wherein said configuring includes publishing information from said central database on an information bus as at least one event, said AAA services subscribing to said event so as to receive said published information so as to thereby update their associated databases.

7. A method in accordance with claim 6, further comprising:

receiving at a protocol gateway in the PoP a network access request from a user through a network access server (NAS);

parsing the network access request for an identification of the user's domain;

routing the network access request to one of said plurality of AAA services at the PoP if the user's domain corresponds to that of the PoP while load balancing among said plurality of AAA services;

looking up a domain identification entry corresponding to the user's domain in one of said plurality of AAA service's databases if the user's domain does not correspond to that of the PoP;

proxying the network access request to an AAA service in the user's domain at an address and port as specified in the domain identification entry of the database if the user's domain does not correspond to that of the PoP.

8. A method in accordance with claim 7, further comprising:

obtaining an IP address for the user from the AAA service in the user's domain if the user's domain does not correspond to that of the PoP.

9. A method in accordance with claim 7, further comprising:

assigning an IP address to the user from a local DHCP pool of IP address if the user's domain does not correspond to that of the PoP.

10. A method in accordance with claim 7, further comprising:

assigning an IP address to the user from an IP address pool identified in an access-accept packet received from the user's domain's AAA service if the user's domain does not correspond to that of the PoP.

11. A method for managing network access to a data communications network, said method comprising:

maintaining a central database, said central database containing access information for authentication, authorization and accounting services associated with domains of the data communications network;

maintaining at a point of presence (PoP) of the data communications network at least one AAA service and at least one proxy service and at least one protocol gateway in communication with a network access server (NAS);

periodically publishing information contained in said central database;

subscribing at said AAA and said proxy service to information published from said central database;

receiving at a protocol gateway in the PoP a network access request from a user through a network access server (NAS);

parsing the network access request at the protocol gateway for an identification of the user's domain;

routing the network access request to an AAA service at the PoP if the user's domain corresponds to that of the PoP;

looking up access information within a domain identification entry corresponding to the user's domain in a database associated with the proxy server if the user's domain does not correspond to that of the PoP; and

proxying the network access request to an AAA service in the user's domain at an address and port as specified in the access information if the user's domain does not correspond to that of the PoP.

12. A method in accordance with claim 11, further comprising:

obtaining an IP address for the user from an AAA service in the user's domain if the user's domain does not correspond to that of the PoP.

13. A method in accordance with claim 11, further comprising:

assigning an IP address to the user from a local DHCP pool of IP address if the user's domain does not correspond to that of the PoP.

14. A method in accordance with claim 11, further comprising:

assigning an IP address to the user from an IP address pool identified in an access-accept packet received from the user's domain's AAA service if the user's domain does not correspond to that of the PoP.

15. A method of managing network access requests to a data communications network, said method comprising:

receiving at a protocol gateway in a point of presence (PoP) of the data communications network a network access request from a user through a network access server (NAS);

parsing the network access request for an identification of the user's domain;

routing the network access request to one of the plurality of authentication, authorization and accounting (AAA) services associated with the PoP if the user's domain corresponds to that of the PoP while load balancing among the plurality of AAA services;

looking up a domain identification entry corresponding to the user's domain in a database if the user's domain does not correspond to that of the PoP;

proxying the network access request via one of a plurality of proxy services to an AAA service in the user's domain at an address and port as specified in the domain identification entry of the database if the user's domain does not correspond to that of the PoP while load balancing among the plurality of proxy services.

16. A method in accordance with claim 15, further comprising:

obtaining an IP address for the user from the AAA service in the user's domain if the user's domain does not correspond to that of the PoP.

17. A method in accordance with claim 15, further comprising:

assigning an IP address to the user from a local DHCP pool of IP address if the user's domain does not correspond to that of the PoP.

18. A method in accordance with claim 15, further comprising:

assigning an IP address to the user from an IP address pool identified in an access-accept packet received from the user's domain's AAA service if the user's domain does not correspond to that of the PoP.

19. A method for managing network access to a data communications network, said method comprising:

maintaining a central database, said central database containing access information for authentication, authorization and accounting services associated with domains of the data communications network;

maintaining at a point of presence (PoP) of the data communications network a plurality of AAA services at least one AAA service and at least one proxy service and at least one protocol gateway in communication with a network access server (NAS);

periodically publishing information contained in said central database;

subscribing at said AAA and said proxy service to information published from said central database;

receiving at a protocol gateway in the PoP a network access request from a user through a network access server (NAS);

parsing the network access request at the protocol gateway for an identification of the user's domain;

routing the network access request to one of said plurality of AAA services at the PoP if the user's domain corresponds to that of the PoP while load balancing among said plurality of AAA services;

looking up access information within a domain identification entry corresponding to the user's domain in a database associated with one of said plurality of proxy services if the user's domain does not correspond to that of the PoP while load balancing among said plurality of proxy services; and

proxying the network access request to an AAA service in the user's domain at an address and port as specified in the access information if the user's domain does not correspond to that of the PoP.

20. A method in accordance with claim 19, further comprising:

obtaining an IP address for the user from an AAA service in the user's domain if the user's domain does not correspond to that of the PoP.

21. A method in accordance with claim 19, further comprising:

assigning an IP address to the user from a local DHCP pool of IP address if the user's domain does not correspond to that of the PoP.

22. A method in accordance with claim 19, further comprising:

assigning an IP address to the user from an IP address pool identified in an access-accept packet received from the user's domain's AAA service if the user's domain does not correspond to that of the PoP.

23. A method of managing network access requests to a data communications network, said method comprising:

receiving at a protocol gateway in a point of presence (PoP) of the data communications network a network access request from a user through a network access server (NAS);

parsing the network access request for an identification of the user's domain;

routing the network access request to an authentication, authorization and accounting (AAA) service associated with the PoP if the user's domain corresponds to that of the PoP;

looking up a domain identification entry corresponding to the user's domain in a database if the user's domain does not correspond to that of the PoP;

proxying the network access request to an AAA service in the user's domain at an address and port as specified in the domain identification entry of the database if the user's domain does not correspond to that of the PoP.

24. A method in accordance with claim 1, further comprising:

obtaining an IP address for the user from the AAA service in the user's domain if the user's domain does not correspond to that of the PoP.

25. A method in accordance with claim 1, further comprising:

assigning an IP address to the user from a local DHCP pool of IP address if the user's domain does not correspond to that of the PoP.

26. A method in accordance with claim 1, further comprising:

assigning an IP address to the user from an IP address pool identified in an access-accept packet received from the user's domain's AAA service if the user's domain does not correspond to that of the PoP.

27. A system for data communications network access management, comprising:

a central database containing information identifying access information for authentication, authorization and accounting (AAA) services associated with domains of the data communications network;

a publisher, said publisher publishing information from said central database to subscribers over an information bus;

a point of presence (PoP) on the data communications network, said PoP including a protocol gateway in communication with at least one network access server (NAS);

an AAA service associated with said PoP and in communication with said protocol gateway, said AAA service subscribing to information published by said publisher; and

a proxy service associated with the PoP and in communication with said protocol gateway, said proxy service subscribing to information published by said publisher,

said protocol gateway receiving network access requests from users over the NAS, parsing the requests for domain identification and routing the requests for domains other than those associated with the PoP to the proxy service,

said proxy service routing network access requests to AAA services in remote domains in accordance with said access information.

28. A system in accordance with claim 27, further comprising: an AAA database associated with said AAA service; and a proxy database associated with said proxy service,

said AAA database populated at instantiation of said AAA service by receiving information published by said publisher from said central database,

said proxy database populated at instantiation of said proxy service by receiving information published by said publisher from said database.

29. A system for data communications network access management, comprising:

a central database containing information identifying access information for authentication, authorization and accounting (AAA) services associated with domains of the data communications network;

a publisher, said publisher publishing information from said central database to subscribers over an information bus;

a point of presence (PoP) on the data communications network, said PoP including a protocol gateway in communication with at least one network access server (NAS);

a plurality of AAA services associated with said PoP and in communication with said protocol gateway, said AAA services subscribing to information published by said publisher; and

a plurality of proxy services associated with said PoP and in communication with said protocol gateway, said proxy services subscribing to information published by said publisher,

said protocol gateway receiving network access requests from users over the NAS, parsing the requests for domain identification and routing the requests for domains other than those associated with the PoP to one of said plurality of proxy services while load balancing among them,

said proxy service routing network access requests to AAA services in remote domains in accordance with said access information.

30. A system in accordance with claim 29, further comprising:

a plurality of AAA databases associated with said respective AAA services; and

a plurality of proxy databases associated with said respective proxy services,

said AAA databases populated at instantiation of said respective AAA services by receiving information published by said publisher from said central database,

said proxy databases populated at instantiation of said respective proxy services by receiving information published by said publisher from said database.

* * * * *